UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/517,134	12/06/2004	Junbiao Zhang	PU020267	6840

7590 06/19/2009

Joseph S Tripoli
Thomson Licensing Inc
PO Box 5312
Princeton, NJ 08543-5312

EXAMINER	
OKORONKWO, CHINWENDU C	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
06/19/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/517,134	ZHANG, JUNBIAO	
	Examiner	Art Unit	
	CHINWENDU C. OKORONKWO	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 March 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. In response to communications filed on 03/06/2009, the Examiner acknowledges the amendments made to the claims and have both considered and applied them to the claims.

Claims 1-18 are presented for examination.

Response to Remarks/Arguments

2. Applicant's arguments with respect to the rejection of the claims have been fully considered but they are moot in view of the new ground(s) of rejection.

2.1 In response to Applicant argument regarding the 101 rejection of claims 16-18, the Examiner has reconsidered the claim language and has withdrawn the rejection, due to the recitation of a "first network" which by definition is a series of electronic devices (tangible matter - hardware) linked by some means of connection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brown et al. (US Patent No. 5,689,563 *hereinafter* "Brown") and further Faccin et al. (US Patent No. 6,879,690 B2 *hereinafter* "Faccin")

Regarding claim 1, Brown, discloses a wireless LAN (WLAN) having an interworking function, a method for interworking between the WLAN and a second network, the WLAN and the second network capable of communicating with a broker, the method comprising the steps of:

- receiving from the broker (5:18 – "subscriber communication unit 100 is comprised of a microprocessing stage 118"), a first key (5:18-52 –"which performs many of the preferred embodiment authentication and encryption steps by accessing a non-volatile memory unit 106 … memory unit 106 also serves as a storage location for keys generated by the encryption/decryption device 120. These keys may include first shared secret data 112 (SSD.sub.A)");
- receiving from a user device, a second network to user certificate that includes a broker to second network certificate and a second key (5:34-52 –"The serial number 110 is used as a second subscriber unit Identifier which is known only to the subscriber unit and the fixed network unit" and " memory unit 106 also serves as a storage location for keys generated by the encryption/decryption device 120. These keys may include … second shared secret data 114 (SSD.sub.B)");

- generating a session key, encrypting the session key using the second key, and transmitting the encrypted session key to the user device (3:66—4:5 – "a session key is generated as a function of the first shared-secret data, the second shared-secret data, the random challenge, and the instant-specific information"); and
- communicating with the user device using the session key (6:54-64 – "if the communicated authentication message is authentic, then the authenticating unit grants further communication between the subscriber unit 100 and the communication unit 130 by recovering 218 the dialed digits which uniquely identifies the target communication unit and the second subscriber unit identifier by decrypting the communicated encrypted data be using the session key as an decryption variable and establishing 220 a communication link").

Although Brown is silent in disclosing the following limitations, Faccin does disclose such limitations which include:

- authenticating the broker to second network certificate using the first key to derive a third key (2:35-36 – "generate the third key using the first key and the second random number") ;
- authenticating the second network to user certificate using the third key to derive the second key (2:54-57 – "update (generate) the second key with the third key");

It would have been obvious for one of ordinary skill in the art to have been motivated to combine the method and apparatus for efficient real-time authentication and encryption of Brown with the method and system for delegation of security procedures to a visited domain of Faccin, as both are directed towards authentication of a mobile node or device with a domain network or network server. The motivation for this combination is provided in the recitation, "a need exists for method and apparatus that allows a user/mobile node and a visited network to perform authentication and key distribution procedures without requiring many round trip communications between the visited network and the home domain network of the user, and that provides a local security association (LSA) that allows for optimizations and empowers a visited network to authenticate a user at any time, as well as empowers the user to authenticate the network at any time (2:4-14 of Faccin)."

Regarding claim 2, Brown, discloses the second network to user certificate further including a subscription level of the user that indicates whether the user is subscribed for an interworking service, and the generating step is performed in response to the subscription level (4:5-11 – "expected authentication message is generated as a function of the first shared-secret data, the random challenge,

and the instant-specific information." and 7:38-47 – "instant-specific information may include one or more of the following types of information including a time of day, radio frequency carrier frequency, a time slot number, a radio port number, access manager identifier, a radio port control unit identifier, and a base site controller identifier").

Although Brown is silent in disclosing claim 3, Faccin does disclose the limitations of claim 3, which include:

- the second network to user certificate further includes an expiration time of the second network to user certificate, and the method further comprises the step of checking the expiration time to determine whether the second network to user certificate has expired (7:34-41 – "temporary shared key may be updated if the temporary shared key previously established and distributed to the user and visited domain has expired ... or the temporary shared key was previously used in a different visited domain and for the sake of security it is the policy").

Regarding claim 4, Brown, the method of claim 1, further including the step of generating a WLAN to user certificate that is signed with a fifth key and includes the session key, whereby the user device is able to authenticate the WLAN (4:24-39 – "methods and apparatus for authentication of mobile nodes and networks").

Claim 5 is disclosed by Brown and is rejected under the same rationale as claim 1, as both claims comprise similar limitations.

Claim 6 is disclosed by Faccin in view of Brown and is rejected under the same rationale as claim 2, as both claims comprise similar limitations.

Claim 7 is disclosed by Brown and is rejected under the same rationale as claim 3, as both claims comprise similar limitations.

Claim 8 is disclosed by Brown and is rejected under the same rationale as claim 4, as both claims comprise similar limitations.

Claim 9 is disclosed by Brown and is rejected under the same rationale as claim 1, as both claims comprise similar limitations.

Claim 10 is disclosed by Brown and is rejected under the same rationale as claim 1, as both claims comprise similar limitations.

Claim 11 is disclosed by Faccin in view of Brown and is rejected under the same rationale as claim 2, as both claims comprise similar limitations.

Claim 12 is disclosed by Brown and is rejected under the same rationale as claim 3, as both claims comprise similar limitations.

Claim 13 is disclosed by Brown and is rejected under the same rationale as claim 4, as both claims comprise similar limitations.

Regarding claim 14, Brown, discloses a broker based system for authenticating users in networks having interworking relationships, comprising:

- a wireless LAN (WLAN) having an interworking function (Fig. 1 and 4:31-49 – "mobile node and its home domain ... visited domain");
- a second network (4:40-49 – "visited domain"); and
- a broker capable of communicating with the WLAN and the second network, the broker (5:18 – "subscriber communication unit 100 is comprised of a microprocessing stage 118") having means for transmitting a broker public key to the WLAN, and means for transmitting a broker to second network certificate, which is signed with a broker private key and includes a second network public key, to the second network (4:51-67 and 5:3-11), the second network including means for transmitting, to a user device, a second network to user certificate signed with a second network private key and includes the broker to second network certificate and the user public key, the WLAN including means for authenticating the broker to second network certificate and deriving the second network public key,

means for authenticating the second network to user certificate and deriving the user public key, and means for generating a session key and encrypting the session key with the user public key (Fig. 2 and 5:12-52).

Regarding claim 15, Brown, discloses the method of claim 14, wherein the WLAN further includes means for transmitting a WLAN to user certificate signed with a WLAN private key and includes the encrypted session key (5:12-52 – "exchange information in a secure and mutually authenticated fashion in the two networks").

Regarding claim 16, Brown, discloses a mobile device comprising: means for receiving from a second network a second network to user certificate that includes

- a broker to second network certificate and a key (5:34-52);
- means for transmitting said second network to user certificate to a first network (5:34-52);
- means for receiving a session key generated by said first network (3:66—4:5); and

  means for communicating with said first network using said session key (6:54-64).

Regarding claim 17, Brown, discloses the mobile device according to claim 16, wherein said first network is a wireless local area network having an interworking function (4:5-11).

Regarding claim 18, Brown, discloses the mobile device according to claim 16, wherein said second network is a cellular network (1:17-37 – "cellular phones … mobile device/node roams … visited domain (network) and home domain (network)").

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHINWENDU C. OKORONKWO whose telephone number is (571)272-2662. The examiner can normally be reached on MWF 2:30 - 6:00, TR 9:00-3:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. C. O./
Examiner, Art Unit 2436

/David García Cervetti/
Primary Examiner, Art Unit 2436